JOURNAL OF NUMBER THEORY 24, 70–88 (1986)

Approximation Lattices of p-adic Numbers

B. M. M. DE WEGER

Mathematisch Instituut R.U.L.,
P.O. Box 9512, 2300 RA Leiden, The Netherlands

Communicated by D. J. Lewis

Received September 26, 1984

Approximation lattices occur in a natural way in the study of rational approximations to p-adic numbers. Periodicity of a sequence of approximation lattices is shown to occur for rational and quadratic p-adic numbers, and for those only, thus establishing a p-adic analogue of Lagrange's theorem on periodic continued fractions. Using approximation lattices we derive upper and lower bounds for the best approximations to a p-adic number, thus establishing the p-adic analogue of a theorem of Hurwitz. © 1986 Academic Press, Inc.

1. INTRODUCTION

The applications of p-adic approximations to finding all solutions of a diophantine equation (cf. [1]), to error-free computation by the so-called Hensel-codes using a computer (cf. [9]), and to the factorization of polynomials (cf. [15]) lead to the following questions. How well can a p-adic number be approximated by rational numbers? Does there exist an efficient algorithm to compute the best rational approximations to any p-adic number? Mahler [10], Schneider [13], Bundschuh [4], and Browkin [3] considered the second question by generalizing the theory of real continued fractions to the p-adic case in various ways. In the real case the best rational approximations to some real number α are just the convergents from the simple continued fraction expansion of α. It turns out that in the proposed p-adic analogues many convergents are bad approximations, and it seems that a simple and satisfactory p-adic continued fraction algorithm does not exist.

A third question is whether there exists a p-adic analogue of the theorem of Lagrange, which states that the simple continued fraction expansion of a real number α is periodic if and only if α is quadratic irrational. This result plays a vital role in real diophantine approximation theory. Analogous theorems have been obtained for some local fields by Browkin [3] and Harringer [8], and in the p-adic case there are partial results by Browkin [3], Bundschuh [4], Deanin [7], Harringer [8], and Mahler [11].

0022-314X/86 $3.00

In this paper we study these three questions using the concept of approximation lattices of a p-adic number, motivated mainly by two publications of Mahler [11; 12, Chap. 4]. For a p-adic number α and a positive rational integer m, consider the lattice Γ_m of all pairs of rational integers (P, Q) such that $|P-Q\alpha|_p \leqslant p^{-m}$. In Section 2 we observe that there is a correspondence between p-adic integers and sequences of approximation lattices. Periodicity of a sequence of approximation lattices is introduced. The third question is then answered in the affirmative in Theorem 2.1. In Section 3 best approximations with respect to a convex norm Φ are introduced, and an algorithm to compute them is presented. It is a variant of the euclidean algorithm, in this p-adic context for the first time proposed by Mahler [12, Chap. 4]. Thus the second question is answered. In Section 4 we derive p-adic analogues of the following well-known results in the real case. Let α be a real number, and p/q a rational number. If p/q is a best approximation to α, then $|\alpha - p/q| \leqslant q^{-2}$. If $|\alpha - p/q| \leqslant (2q^2)^{-1}$, then p/q is a best approximation to α. If α is irrational, then there are infinitely many solutions p/q of the inequality $|\alpha - p/q| \leqslant (\sqrt{5}q^2)^{-1}$. The constants that occur in the p-adic case are well-known lattice constants depending on the norm Φ. The obtained constants are shown to be best possible, using an ingenious lemma of Tijdeman on the approximation of real matrices by integral ones. This answers the first question. Finally in Section 5 we study periodicity of a sequence of Φ-reduced bases of approximation lattices of a p-adic number α, where Φ is a norm. It is shown that, depending on α and Φ, this periodicity may occur for rational and elliptic α, but does not occur for hyperbolic α.

2. Approximation Lattices and Periodicity

Let p be a prime number, and let $\alpha \in \mathbb{Q}_p$. Put

$$\alpha = \sum_{i=k}^{\infty} a_i p^i, \qquad \alpha_m = \sum_{i=k}^{m-1} a_i p^i$$

for all $m \in \mathbb{Z}$, where $k = \operatorname{ord}_p(\alpha)$, and $a_i \in \{0, 1, \ldots, p-1\}$ for $i = k, k+1, \ldots$. Put $a_i = 0$ for $i = k-1, k-2, \ldots$.

Definition 2.1. (i) The ordered pair of rational integers (P, Q) is called a *p-adic approximation to α of order m* if $|P - Q\alpha|_p = p^{-m}$.

(ii) The set

$$\Gamma_m = \{(P, Q) \in \mathbb{Z}^2 : |P - Q\alpha|_p \leqslant p^{-m}\}$$

is called the mth *approximation lattice of α*.

The structures of the sequences of approximation lattices of α and α^{-1} do not differ essentially. Hence we may assume that $\alpha \in \mathbb{Z}_p$. Then $\alpha_m \in \mathbb{Z}$, and $p^k \mid \alpha_m$ for $m = 0, 1, 2, \ldots$. The approximation lattices satisfy the following properties. The proofs are left to the reader.

LEMMA 2.1. (i) *Γ_m is a lattice in $\mathbb{Z}^2$ of rank 2.*

(ii) $\Gamma_0 = \mathbb{Z}^2$.

(iii) $\Gamma_{m+1} \subset \Gamma_m$.

(iv) *The index of Γ_{m+1} in Γ_m, defined as $\#(\Gamma_m/\Gamma_{m+1})$, is p.*

(v) $\det(\Gamma_m) = p^m$.

(vi) *A pair of points $\{(P, Q), (R, S)\}$ in Γ_m is a basis of Γ_m if and only if $|PS - QR| = p^m$.*

(vii) *$\{(p^m, 0), (\alpha_m, 1)\}$ is a basis of Γ_m.*

Let $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2 \supset \cdots$, be an infinite sequence of lattices in $\mathbb{R}^2$.

DEFINITION 2.2. The sequence $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2 \supset \cdots$, is said to be *of index p* if the index of Λ_{m+1} in Λ_m is p for all $m \geqslant 0$. It is called *irreducible* if $\Lambda_{m+1} \neq p\Lambda_{m-1}$ for all $m \geqslant 1$.

Let $\alpha \in \mathbb{Z}_p$. By Lemma 2.1 the sequence of approximation lattices $\{\Gamma_m\}_{m=0}^{\infty}$ of α is of index p and irreducible. We investigate the relation of p-adic numbers and sequences of lattices a little further. Let for any lattice Λ the *inverse lattice* Λ^{-1} be defined by interchanging coordinates. Let $\mathbb{Z}^2 = \Lambda_0 \supset \Lambda_1 \supset \Lambda_2 \supset \cdots$, be of index p and irreducible. Then the same is true for the sequence of inverse lattices $\mathbb{Z}^2 = \Lambda_0^{-1} \supset \Lambda_1^{-1} \supset \Lambda_2^{-1} \supset \cdots$. Let $\{(P, Q), (R, S)\}$ be a basis of Λ_1 with $PS - QR = p$. Then $\gcd(P, R) = 1$ or $\gcd(Q, S) = 1$. By considering inverse lattices if necessary, we may suppose that the latter holds. It then follows easily that for every $m \geqslant 0$ there exists a $\beta_m \in \mathbb{Z}$ with $0 \leqslant \beta_m \leqslant p^m - 1$, such that $\{(p^m, 0), (\beta_m, 1)\}$ is a basis of Λ_m. Observe that

$$\beta = \lim_{m \to \infty} \beta_m$$

exists in $\mathbb{Z}_p$ (throughout this section we denote by lim the p-adic limit). Then Λ_m is the mth approximation lattice of β. If $\operatorname{ord}_p(\beta) = 0$, then Λ_m^{-1} is the mth approximation lattice of β^{-1}. If $\operatorname{ord}_p(\beta) = k > 0$, then Λ_m^{-1} is the $(m-k)$th approximation lattice of β^{-1} for $m \geqslant k$. Thus we have the following result.

FUNDAMENTAL OBSERVATION. *There is a one-to-one correspondence between the ring of p-adic integers $\mathbb{Z}_p$ and the set of sequences of lattices*

$\mathbb{Z}^2 = \Lambda_0 \supset \Lambda_1 \supset \Lambda_2 \supset \cdots$, *that are of index* p, *irreducible, and for which any basis* $\{(P, Q), (R, S)\}$ *of* Λ_1 *satisfies* $\gcd(Q, S) = 1$.

DEFINITION 2.3. Let $\alpha \in \mathbb{Z}_p$. The sequence of approximation lattices $\{\Gamma_m\}_{m=0}^{\infty}$ of α is called *periodic* if there exist rational integers $k > 0$, $m_0 \geqslant 0$, and a linear mapping $\Xi\colon \mathbb{R}^2 \to \mathbb{R}^2$ such that $\Xi(\Gamma_m) = \Gamma_{m+k}$ for all $m \geqslant m_0$.

Remark. Choose in each Γ_m a basis $\{(P_m, Q_m), (R_m, S_m)\}$, and put

$$C_m = \begin{pmatrix} P_m & Q_m \\ R_m & S_m \end{pmatrix}.$$

Let χ^{T} be the matrix of Ξ. Periodicity of $\{\Gamma_m\}_{m=0}^{\infty}$ now means that for $m \geqslant m_0$ the basis of Γ_m can be chosen so that $C_{m+k} = C_m \chi$. Define for $m = 0, 1, 2, \ldots$, matrices ψ_m by $C_{m+1} = \psi_m C_m$. By Lemma 2.1(iii), ψ_m is integral. We have for $m \geqslant m_0$,

$$\psi_{m+k} C_{m+k} = C_{m+k+1} = C_{m+1}\chi = \psi_m C_m \chi = \psi_m C_{m+k},$$

hence the sequence $\{\psi_m\}_{m=0}^{\infty}$ is periodic if the sequence of lattices is periodic. Conversely, if for some sequence of approximation lattices $\{\Gamma_m\}_{m=0}^{\infty}$ the bases can be chosen such that the sequence $\{\psi_m\}_{m=0}^{\infty}$ is periodic, then the sequence of lattices is periodic. For, if we define for $m \geqslant m_0$ the matrix χ_m by $C_{m+k} = C_m \chi_m$, then we have

$$C_{m+1}\chi_{m+1} = C_{m+k+1} = \psi_{m+k} C_{m+k} = \psi_m C_m \chi_m = C_{m+1}\chi_m,$$

hence all χ_m are equal for $m \geqslant m_0$.

THEOREM 2.1. *Let* p *be prime, and* $\alpha \in \mathbb{Z}_p$. *Its sequence of approximation lattices is periodic if and only if* α *is algebraic of degree at most* 2.

Proof. Let $\{\Gamma_m\}_{m=0}^{\infty}$ be the periodic sequence of approximation lattices of α. Let k, m_0, Ξ, χ, and C_m be as above. Put

$$\chi = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}.$$

Note that $\det(\chi) = \pm p^k$, and $x_{ij} \in p^{-h}\mathbb{Z}$ $(i, j = 1, 2)$ for some rational integer $h \geqslant 0$. Fix an $m_1 \geqslant m_0$. Then $C_{m_1+nk} = C_{m_1}\chi^n$ for $n = 0, 1, 2, \ldots$. From

$$\chi^2 = \mathrm{Tr}(\chi)\chi - \det(\chi) I$$

we obtain

$$C_{m_1+2k} \equiv \mathrm{Tr}(\chi) C_{m_1+k} \pmod{p^k}.$$

Hence, by the irreducibility of the sequence of approximation lattices, we infer $\mathrm{ord}_p(\mathrm{Tr}(\chi))=0$. Since the denominator of $\mathrm{Tr}(\chi)$ is a power of p, this implies $\mathrm{Tr}(\chi)\in\mathbb{Z}$. Since C_{m_1+nk} corresponds to a basis of the (m_1+nk)th approximation lattice of α, we have

$$C_{m_1+nk}\mathbf{v}\equiv\mathbf{0}(\mathrm{mod}\ p^{m_1+nk})$$

with $\mathbf{v}=\binom{1}{-\alpha}$. Hence

$$\lim_{n\to\infty} C_{m_1}\chi^n\mathbf{v}=\mathbf{0}. \tag{1}$$

We claim that $\mathbf{v}$ is an eigenvector of Ξ. The eigenvalues ϕ, $\bar{\phi}$ of Ξ satisfy

$$x^2-\mathrm{Tr}(\chi)x\pm p^k=0.$$

By $\mathrm{ord}_p(\phi+\bar{\phi})=\mathrm{ord}_p(\mathrm{Tr}(\chi))=0$ $\mathrm{ord}_p(\phi\bar{\phi})=k$ we may assume $\mathrm{ord}_p(\phi)=k$, $\mathrm{ord}_p(\bar{\phi})=0$. With respect to a suitably chosen basis of $\mathbb{R}^2$ the matrix of Ξ becomes

$$\begin{pmatrix}\phi & 0\\ 0 & \bar{\phi}\end{pmatrix}.$$

Let $\mathbf{v}=\binom{v_1}{v_2}$ with respect to this basis. Then

$$\chi^n\mathbf{v}=\begin{pmatrix}\phi^n v_1\\ \bar{\phi}^n v_2\end{pmatrix}.$$

By (1) we have

$$\lim_{n\to\infty}\bar{\phi}^n v_2=0.$$

Thus $v_2=0$, since $\mathrm{ord}_p(\bar{\phi})=0$. It follows that $\Xi\mathbf{v}=\phi\mathbf{v}$, which proves our claim.

Returning to the standard basis of $\mathbb{R}^2$, we have

$$\chi\mathbf{v}=\begin{pmatrix}x_{11}-x_{12}\alpha\\ x_{21}-x_{22}\alpha\end{pmatrix}=\begin{pmatrix}\phi\\ -\phi\alpha\end{pmatrix}.$$

Eliminating ϕ we obtain

$$x_{12}\alpha^2-(x_{11}-x_{22})\alpha-x_{21}=0.$$

Since $x_{ij}\in\mathbb{Q}$ $(i,j=1,2)$ it follows that α is algebraic of degree at most 2.

To prove the if-part of the theorem, first suppose that α is rational, $\alpha=P/Q$ say, with $P, Q\in\mathbb{Z}$, $\gcd(P,Q)=1$. Let $R, S\in\mathbb{Z}$ satisfy $PS-QR=1$.

Since $\alpha \in \mathbb{Z}_p$, p does not divide Q. Hence $\gcd(Q, S) = 1$. It follows that $\{(P, Q), (p^m R, p^m S)\}$ is a basis of Γ_m for all $m \geqslant 0$. Periodicity follows by choosing

$$\psi_m = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$$

for all $m \geqslant 0$, using the remark following Definition 2.3.

Next suppose that α is quadratic irrational, say that

$$a\alpha^2 + b\alpha + c = 0$$

holds, with $a, b, c \in \mathbb{Z}$ relatively prime, and $d = b^2 - 4ac$ not a square. Put $h = \frac{1}{2} \operatorname{ord}_p(d)$ and $d' = dp^{-2h}$. In order that $\alpha \in \mathbb{Q}_p$ exists, the following conditions should hold:

(a) $\operatorname{ord}_p(d)$ is even (so $h \in \mathbb{Z}$),

(b) d' is a quadratic residue (mod p) if p is odd,

(c) $d' \equiv 1 \pmod 8$ if $p = 2$.

Choose $e \in \mathbb{Z}$ such that $\operatorname{ord}_p(e + a\alpha) = h$ if $h > 0$, and $e = 0$ if $h = 0$. Put $\eta = p^{-h}(e + a\alpha)$. Since $2a\alpha = -b + \sqrt{d}$ we find that η is an algebraic integer. Let $\mathcal{O}$ be the quadratic order generated by 1 and η (for the theory of quadratic orders see [2, Chap. 2]). The discriminant of $\mathcal{O}$ is d', which is not divisible by p. Put

$$\mathfrak{p} = \{\xi \in \mathcal{O} : |\xi|_p \leqslant p^{-1}\}.$$

This is a prime ideal in $\mathcal{O}$ lying above p. We have for $m = 1, 2, 3, \ldots$,

$$\mathfrak{p}^m = \{\xi \in \mathcal{O} : |\xi|_p \leqslant p^{-m}\}.$$

If $m \geqslant 2h + 1$, then the mth approximation lattice Γ_m of α is related to $\mathfrak{p}^{m-h}$ as follows:

$$\Gamma_m = \{(P, Q) \in \mathbb{Z}^2 : p^{-h}(Pa + Qe) - Q\eta \in \mathfrak{p}^{m-h}\} \tag{2}$$

(note that $Pa + Qe \equiv 0 \pmod{p^h}$ since $P \equiv Q\alpha \pmod{p^m}$). Choose a rational integer $k \geqslant 1$ such that $\mathfrak{p}^k$ is principal, say $\mathfrak{p}^k = (\phi)$, with $\phi \in \mathcal{O}$. By (2), the linear mapping $\mathfrak{p}^m \to \mathfrak{p}^{m+k}$ defined by $\xi \to \phi\xi$ induces a linear mapping $\Xi : \mathbb{Z}^2 \to \mathbb{Z}^2$ with

$$\Xi(P, Q) = (P', Q'),$$

$$P' - Q'\alpha = \phi(P - Q\alpha).$$

If $(P, Q) \in \Gamma_m$ then $|P' - Q'\alpha|_p \leqslant p^{-(m+k)}$. We claim that $(P', Q') \in \Gamma_{m+k}$. Put $\phi = x + y\eta$ with $x, y \in \mathbb{Z}$. Then

$$P' = xP + yp^{-h}(Pe + Qc),$$
$$Q' = xQ + yp^{-h}(-Pa + Qe - Qb).$$

Since mod p^h

$$Pe + Qc \equiv Q\alpha(e - a\alpha - b) \equiv -Q\alpha(2a\alpha + b) = -Q\alpha\sqrt{d} \equiv 0,$$
$$-Pa + Qe - Qb \equiv -Q(2a\alpha + b) = -Q\sqrt{d} \equiv 0$$

we have $P', Q' \in \mathbb{Z}$. Thus $(P', Q') \in \Gamma_{m+k}$. It follows that $\Xi(\Gamma_m) = \Gamma_{m+k}$. ∎

3. Convex Norms and Best Approximations

The function $\Phi: \mathbb{R}^2 \to \mathbb{R}$ is called a (*convex*) *norm* if

(i) $\Phi(X, Y) \geqslant 0$ for all $(X, Y) \in \mathbb{R}^2$,

(ii) $\Phi(X, Y) = 0$ if and only if $(X, Y) = (0, 0)$,

(iii) $\Phi(tX, tY) = |t|\,\Phi(X, Y)$ for all $(X, Y) \in \mathbb{R}^2$, $t \in \mathbb{R}$,

(iv) $\Phi(X_1 + X_2, Y_1 + Y_2) \leqslant \Phi(X_1, Y_1) + \Phi(X_2, Y_2)$ for all (X_1, Y_1), $(X_2, Y_2) \in \mathbb{R}^2$.

Two examples that occur frequently in the literature are the *square norm* $\Phi_M(X, Y) = \max(|X|, |Y|)$, and the *euclidean norm* $\Phi_E(X, Y) = (X^2 + Y^2)^{1/2}$.

In any lattice $\Lambda \subset \mathbb{R}^2$ there is at least one nonzero point (P, Q) with minimal norm Φ, a so-called *first successive minimal point of* Λ. Fix such a (P, Q). In the set of lattice points that are independent of (P, Q) there is a point with minimal Φ, a *second successive minimal point of* Λ. Two successive minimal points can be found such that they form a basis of Λ, a so-called Φ-*reduced* basis. We apply this to approximation lattices of p-adic numbers.

Definition 3.1. Let $\alpha \in \mathbb{Z}_p$, let Φ be a norm. The nonzero pair of rational integers (P, Q) is called a *nearly* Φ-*best approximation to* α if all nonzero approximations to α of smaller norm than (P, Q) have smaller approximation order than (P, Q). A nearly Φ-best approximation (P, Q) to α is said to be a Φ-*best approximation to* α if all approximations to α of norm equal to that of (P, Q) have approximation order at least that of (P, Q).

It follows immediately that a nearly Φ-best approximation to α of order m is a first successive minimal point in Γ_m (and possibly also in some other

approximation lattices of α). Hence it belongs to a Φ-reduced basis of Γ_m. The following algorithm computes a Φ-reduced basis of a lattice $\Lambda \subset \mathbb{R}^2$, starting from any basis.

ALGORITHM. *Let* $\{(X, Y), (Z, U)\}$ *be a basis of* Λ.

(i) *Compute the minimal* $K \in \mathbb{Z}$ *for which* $\Phi(X+KZ, Y+KU)$ *is minimal. Put* $(X, Y) := (X+KZ, Y+KU)$.

(ii) *If* $\Phi(X, Y) < \Phi(Z, U)$ *then interchange* (X, Y) *and* (Z, U), *and go to* (i); *else stop.*

If the p-adic expansion $\sum_{i=0}^{\infty} a_i p^i$ of $\alpha \in \mathbb{Z}_p$ is known completely (or partially), then bases of (some) approximation lattices of α are known by Lemma 2.1(vii). The above algorithm may then be applied to compute Φ-best approximations to α. We do not give the (easy) proof of the correctness of the algorithm. It is essentially the euclidean algorithm. In the context of p-adic approximation theory it is essentially due to Mahler [12, Chap. 4]. It has recently been rediscovered by several authors in different contexts (cf. [9, 16]). It works well in practice to compute good rational approximations to any p-adic number (cf. [1]). For a particular norm Φ, step (i) might be specified. For example, for Φ_M, K is one of the two neighbouring integers of k, where

$$k = -\frac{X-Y}{Z-U} \qquad \text{if} \quad ZU < 0,$$

$$k = -\frac{X+Y}{Z+U} \qquad \text{if} \quad ZU > 0,$$

$$k = \min\left(-\frac{X-Y}{Z-U}, -\frac{X+Y}{Z+U}\right) \qquad \text{if} \quad ZU = 0.$$

For Φ_E, K is the nearest integer to

$$k = -\frac{XZ+YU}{X^2+Y^2}.$$

4. APPROXIMATION THEOREMS

Let Φ be a norm, and p a prime number. We define the p-adic "Hurwitz-constant" $h = h(\Phi, p)$ as the supremum of the $k \in \mathbb{R}$ such that for all irrational $\alpha \in \mathbb{Z}_p$ the inequality

$$|P - Q\alpha|_p \leqslant \frac{1}{k\Phi(P, Q)^2}$$

has infinitely many solutions $(P, Q) \in \mathbb{Z}^2$. For elliptic norms $\Phi(X, Y) = (aX^2 + bXY + cY^2)^{1/2}$ with $b^2 - 4ac = -4$, $h(\Phi, p)$ has been investigated by Mahler [11] and Deanin [6]. Put $h(\Phi) = \inf_p h(\Phi, p)$. Mahler showed that $h(\Phi) = \sqrt{3}/2$ for those elliptic norms. In Theorem 4.1, the main result of this section, we shall prove that $h(\Phi) = \Delta(\Phi)$ for any norm Φ, where $\Delta(\Phi)$ is the *lattice constant* of the convex body

$$B_1(\Phi) = \{(X, Y) \in \mathbb{R}^2 : \Phi(X, Y) \leqslant 1\},$$

i.e., $\Delta(\Phi) = \inf(\det(\Lambda))$ where Λ runs through the set of lattices for which $(0, 0)$ is the only lattice point in the interior of $B_1(\Phi)$ (the so-called $B_1(\Phi)$-*admissible lattices*, cf. [5, p. 80]). For any norm Φ there exists at least one lattice for which the infimum is reached, a so-called *critical lattice*. For example, $\Delta(\Phi_M) = 1$, and a critical lattice is $\mathbb{Z}^2$; $\Delta(\Phi_E) = \sqrt{3}/2$, and a critical lattice is generated by the vertices of any regular hexagon inscribed in the unit circle.

THEOREM 4.1. *Let p be prime, and $\alpha \in \mathbb{Z}_p$. Let Φ be a norm.*

(i) *The inequality*

$$|P - Q\alpha|_p \leqslant \frac{1}{\Delta(\Phi)\,\Phi(P, Q)^2} \tag{3}$$

is satisfied by any nearly Φ-best approximation to α.

(ii) *For any p and any $\alpha \notin \mathbb{Q}$,* (3) *has infinitely many solutions $(P, Q) \in \mathbb{Z}^2$.*

(iii) *For p sufficiently large, assertion* (iii) *becomes false if $\Delta(\Phi)$ is replaced by any larger constant.*

The idea behind the proof of part (iii) is to approximate a critical lattice by an integral lattice. We use the following lemma of Tijdeman, which shows that for any lattice $\Lambda \subset \mathbb{R}^2$ with $\det(\Lambda) = 1$ and for any integer $n \geqslant 2$, there exists a lattice in $\mathbb{Z}^2$ of determinant n which is relatively close to $n^{1/2}\Lambda$.

LEMMA 4.1 (Tijdeman [14]). *Let a, a_1, a_2, a_3, a_4 be real numbers with $a_1 a_4 - a_2 a_3 = 1$ and $|a_i| \leqslant a$ for $i = 1, 2, 3, 4$. Then for every integer $n \geqslant 2$ there exist integers A_1, A_2, A_3, A_4 such that $A_1 A_4 - A_2 A_3 = n$ and*

$$|A_i - a_i n^{1/2}| \leqslant C n^{4/9} (\log n)^{7/9} \qquad (i = 1, 2, 3, 4), \tag{4}$$

where C is a constant depending on a only.

Let $\mathbb{R}^{2,2}$ (resp. $\mathbb{Z}^{2,2}$) be the set of 2×2 matrices with real (resp. integral) entries. We define the norm $\|M\|$ of a matrix $M=(m_{ij})\in\mathbb{R}^{2,2}$ by $\|M\|=\max_{i,j}|m_{ij}|$. We have

$$\|M_1+M_2\|\leqslant\|M_1\|+\|M_2\|,$$

$$\|M_1M_2\|\leqslant 2\,\|M_1\|\,\|M_2\|,$$

$$\|M_1^{-1}\|=\|M\|\,|\det(M)|^{-1}$$

for all $M, M_1, M_2\in\mathbb{R}^{2,2}$ with $\det(M)\neq 0$.

LEMMA 4.2. *Let $a\in\mathbb{R}$, and let $m\in\mathbb{R}^{2,2}$ satisfy $\det(m)=1$ and $\|m\|\leqslant a$. Then for every integer $n\geqslant 2$ there exist $M_1, M_2\in\mathbb{Z}^{2,2}$ with $M_1M_2^{-1}\notin\mathbb{Z}^{2,2}$, $\det(M_1)=\det(M_2)=n$ and*

$$\|M_i-mn^{1/2}\|\leqslant Cn^{4/9}(\log n)^{7/9}\qquad(i=1,2),\tag{5}$$

where C is a constant depending on a only.

Proof. Fix $n\geqslant n_0$, where n_0 is a constant depending on a only. Let C_1 be the constant in (4) when Lemma 4.1 is applied with $2a$ in stead of a. Put $\varepsilon=2C_1n^{-1/18}(\log n)^{7/9}$. Choose n_0 so large that $2\varepsilon<a$. There exists an $m'\in\mathbb{R}^{2,2}$ with $\det(m')=1$ and $\varepsilon<\|m-m'\|<2\varepsilon$. Then $\|m'\|\leqslant\|m\|+2\varepsilon<2a$. By Lemma 4.1 there exist $M_1, M_2\in\mathbb{Z}^{2,2}$ with $\det(M_1)=\det(M_2)=n$ and

$$\|M_1-mn^{1/2}\|\leqslant C_1n^{4/9}(\log n)^{7/9},$$

$$\|M_2-m'n^{1/2}\|\leqslant C_1n^{4/9}(\log n)^{7/9}.$$

It follows that

$$\begin{aligned}\|M_2-mn^{1/2}\|&\leqslant\|M_2-m'n^{1/2}\|+n^{1/2}\,\|m'-m\|\\&<5C_1n^{4/9}(\log n)^{7/9}.\end{aligned}$$

Hence (5) holds with $C=5C_1$. It remains to prove that $M_1M_2^{-1}\notin\mathbb{Z}^{2,2}$. Note that $M_1\neq M_2$, since

$$\begin{aligned}\|M_1-M_2\|&\geqslant\|m-m'\|\,n^{1/2}-\|M_1-mn^{1/2}\|-\|M_2-m'n^{1/2}\|\\&>\varepsilon n^{1/2}-2C_1n^{4/9}(\log n)^{7/9}=0.\end{aligned}$$

Further,

$$\|M_1 M_2^{\ 1} - I\| \leqslant 2\,\|M_2^{-1}\|\,\|M_1 - M_2\| = \frac{2}{n}\,\|M_2\|\,\|M_1 - M_2\|$$

$$\leqslant \frac{2}{n}\,(\|m\|\,n^{1/2} + \|M_2 - mn^{1/2}\|)(\|M_1 - mn^{1/2}\| + \|M_2 - mn^{1/2}\|)$$

$$\leqslant C_2 n^{-1/18}(\log n)^{7/9},$$

where C_2 depends on a only. Choose n_0 so large that $C_2 n^{-1/18}(\log n)^{7/9} < 1$. Then $M_1 M_2^{-1} \notin \mathbb{Z}^{2,2}$.

If $n < n_0$ there obviously is a constant C depending on a only such that M_1, M_2 exist with the required properties. ∎

Proof of Theorem 4.1. (i) This is a trivial consequence of the definitions of $\Delta(\Phi)$ and nearly Φ-best approximations.

(ii) Let for some m_1 a first successive minimal point (P_{m_1}, Q_{m_1}) in Γ_{m_1} be given. Then it satisfies (3). Since $a \notin \mathbb{Q}$ there are only finitely many integral multiples of (P_{m_1}, Q_{m_1}) that satisfy (3). Hence there is an $m_2 > m_1$ for which the first successive minimal points in Γ_{m_2} are not multiples of (P_{m_1}, Q_{m_1}). The proof is completed by induction.

(iii) Let $0 < \varepsilon < \frac{1}{3}$. We shall prove that for every prime $p \geqslant p_0$ there exists a p-adic integer α such that for all $(P, Q) \in \mathbb{Z}^2$ with $(P, Q) \neq (0, 0)$,

$$|P - Q\alpha|_p > \frac{1}{(\Delta(\Phi) + \varepsilon)\,\Phi(P, Q)^2}. \tag{6}$$

Here p_0 is a constant depending on Φ and ε only.

Let Λ be a critical lattice of $\{(X, Y) \in \mathbb{R}^2 : \Phi(X, Y) \leqslant \Delta(\Phi)^{-1/2}\}$. Then $\det(\Lambda) = 1$. There exists a basis $\{(a_1, b_1), (c_1, d_1)\}$ of Λ such that $a_1 d_1 - b_1 c_1 = 1$ and $\Phi(a_1, b_1) = \Phi(c_1, d_1) = \Phi(a_1 + c_1, b_1 + d_1) = \Delta(\Phi)^{-1/2}$, and if Φ is a parallelogram norm, also $\Phi(a_1 - c_1, b_1 - d_1) = \Delta(\Phi)^{-1/2}$ (cf. [5, p. 160]). Put

$$M = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix},$$

then $\det(M) = 1$. Let p_0 be a positive real number to be chosen later, and let $p \geqslant p_0$ be prime. We claim that there exists a sequence $\{L_s\}_{s=0}^{\infty}$ of matrices $L_s \in \mathbb{Z}^{2,2}$ with $L_0 = I$, $\det(L_s) = p^s$, $L_s L_{s-1}^{-1} \in \mathbb{Z}^{2,2}$, $L_s L_{s-2}^{-1} \notin p\mathbb{Z}^{2,2}$, and

$$\|L_s - Mp^{s/2}\| \leqslant C_3\, p^{s/2 - 1/18}(\log p)^{7/9} \tag{7}$$

for all s, where C_3 depends on Φ only. Let $s=1$. From Lemma 4.1 it follows that there exists an $L_1 \in \mathbb{Z}^{2,2}$ with $\det(L_1)=p$ and

$$\|L_1 - Mp^{1/2}\| \leqslant C_4 p^{1/2-1/18}(\log p)^{7/9},$$

where C_4 depends on Φ only. Then (7) with $s=1$ follows by choosing $C_3 \geqslant C_4$. Let $s \geqslant 1$, and suppose the claim has been proved for s. Choose p_0 so large that for $p \geqslant p_0$

$$\|L_s - Mp^{s/2}\| \leqslant \varepsilon p^{s/2}. \tag{8}$$

Then by $\varepsilon < \frac{1}{3}$ and $\|M\| \geqslant \sqrt{2}/2$ we have

$$\begin{aligned}\|ML_s^{-1}p^{s/2}\| &\leqslant 1 + 2\|L_s^{-1}\|\ \|L_s - Mp^{s/2}\| \\ &\leqslant 1 + 2\varepsilon(\|M\| + \varepsilon) < 1 + \|M\|.\end{aligned}$$

Applying Lemma 4.2 to the matrix $ML_s^{-1}p^{s/2}$ we find that there exist matrices $K_1, K_2 \in \mathbb{Z}^{2,2}$ with $\det(K_1) = \det(K_2) = p$, $K_1K_2^{-1} \notin \mathbb{Z}^{2,2}$ and

$$\|K_i - ML_s^{-1}p^{(s+1)/2}\| \leqslant C_5 p^{1/2-1/18}(\log p)^{7/9} \qquad (i=1,2), \tag{9}$$

where C_5 depends on Φ only. By $K_1K_2^{-1} \notin \mathbb{Z}^{2,2}$ there exists an $i_0 \in \{1,2\}$ such that $K_{i_0}L_sL_{s-1}^{-1} \notin p\mathbb{Z}^{2,2}$. Put $L_{s+1} = K_{i_0}L_s$. To prove (7) with s replaced by $s+1$, note that, by (9) and (8),

$$\begin{aligned}\|L_{s+1} - Mp^{(s+1)/2}\| &\leqslant 2\ \|L_s\|\ \|K_{i_0} - ML_s^{-1}p^{(s+1)/2}\| \\ &\leqslant 2(\|M\| + \varepsilon)\ p^{s/2}C_5 p^{1/2-1/18}(\log p)^{7/9}.\end{aligned}$$

Now our claim follows by choosing $C_3 \geqslant 2(\|M\| + \frac{1}{3})C_5$.

Put for all $s \geqslant 0$

$$L_s = \begin{pmatrix} P_s & Q_s \\ R_s & S_s \end{pmatrix},$$

and let Λ_s be the lattice generated by $\{(P_s, Q_s), (R_s, S_s)\}$. Then the sequence $\{\Lambda_s\}_{s=0}^{\infty}$ is of index p. It is also irreducible, since $L_sL_{s-2}^{-1} \notin p\mathbb{Z}^{2,2}$ for all $s \geqslant 2$. Without loss of generality we may consider the Λ_s^{-1} instead of the Λ_s, if necessary. By the fundamental observation in Section 2 the sequence $\{\Lambda_s\}_{s=0}^{\infty}$ defines a p-adic integer α. Let $(P, Q) \neq (0, 0)$ be a pair of rational integers, and put $|P - Q\alpha|_p = p^{-m}$. There exist $k, l \in \mathbb{Z}$, $(k, l) \neq (0, 0)$, such that

$$(P, Q) = k(P_m, Q_m) + l(R_m, S_m).$$

Put

$$(a, b) = k(a_1, b_1) + l(c_1, d_1).$$

Note that there is a constant C_6, depending on Φ only, such that for all $(X, Y) \in \mathbb{R}^2$

$$\Phi(X, Y) \leqslant C_6 \max(|X|, |Y|).$$

Hence,

$$\begin{aligned}
&|\Phi(P, Q) - p^{m/2}\Phi(a, b)| \\
&\quad \leqslant \Phi(P - p^{m/2}a, Q - p^{m/2}b) \\
&\quad \leqslant C_6 \max(|P - p^{m/2}a|, |Q - p^{m/2}b|) \\
&\quad \leqslant C_6 \max(|k|\,|P_m - p^{m/2}a_1| + |l|\,|R_m - p^{m/2}c_1|, \\
&\qquad |k|\,|Q_m - p^{m/2}b_1| + |l|\,|S_m - p^{m/2}d_1|).
\end{aligned}$$

Thus, by (7),

$$|\Phi(P, Q) - p^{m/2}\Phi(a, b)| \leqslant C_7(|k| + |l|)\, p^{m/2 - 1/18}(\log p)^{7/9}, \tag{10}$$

where C_7 depends on Φ only. For $\pm(k, l) = (1, 0)$, $(0, 1)$, $(1, 1)$, and $(-1, 1)$ if Φ is a parallelogram norm, we have $\Phi(a, b) = \Delta(\Phi)^{-1/2}$. Then (6) follows from (10) if p_0 is chosen large enough. Since Λ is a critical lattice, there exist positive constants C_8 and C_9, depending on Φ only, such that for all other $(k, l) \neq (0, 0)$

$$\Phi(a, b) > (1 + C_8)\, \Delta(\Phi)^{-1/2}, \tag{11}$$

$$\Phi(a, b) > C_9(|k| + |l|)\, \Delta(\Phi)^{-1/2}, \tag{12}$$

(cf. [5, p. 160]). By choosing p_0 large enough, (6) follows from (10) and (11) if $|k| + |l|$ is small, and from (10) and (12) otherwise. ∎

To conclude this section, we give a criterion for an approximation to be nearly Φ-best. Let Φ be a norm. Define $c(\Phi) = \sup(\det(\Lambda))$, where Λ runs through the set of lattices with two independent points in $B_1(\Phi)$. For any norm Φ there exists at least one lattice for which the supremum is reached. For example, $c(\Phi_M) = 2$, and the supremum is reached for the lattice generated by $(1, 1)$ and $(-1, 1)$; $c(\Phi_E) = 1$, and the supremum is reached for any lattice generated by the vertices of a square inscribed in the unit circle.

THEOREM 4.2. *Let p be prime, and $\alpha \in \mathbb{Z}_p$. Let Φ be a norm.*

(i) *Let (P, Q) be a nonzero pair of rational integers with* $\gcd(P, Q) = 1$, *such that*

$$|P - Q\alpha|_p \leqslant \frac{1}{c(\Phi)\, \Phi(P, Q)^2}. \tag{13}$$

Then (P, Q) is a nearly Φ-best approximation to α.

(ii) *In general,* (i) *becomes false if* $c(\Phi)$ *is replaced by any smaller constant.*

Proof. (i) Let (P, Q) satisfy (13). Put $|P-Q\alpha|_p = p^{-m}$. Let (P', Q') be a nonzero lattice point in Γ_m. We have to prove that $\Phi(P', Q') \geqslant \Phi(P, Q)$. If (P', Q') is an integral multiple of (P, Q), this is trivial. Thus assume $P'Q - PQ' \neq 0$. Then, by $p^m \mid P'Q - PQ'$, we have

$$p^m \leqslant |P'Q - PQ'| \leqslant c(\Phi)\, \Phi(P, Q)\, \Phi(P', Q').$$

Combined with (13) this yields the result.

(ii) Let $\varepsilon > 0$. We shall prove that for any integer $m \geqslant m_0$ there exist a p-adic integer α and an approximation (P, Q) to α, which is not a nearly Φ-best approximation to α, such that

$$|P - Q\alpha|_p \leqslant \frac{1}{(c(\Phi) - \varepsilon)\, \Phi(P, Q)^2}. \tag{14}$$

Here m_0 is a constant depending on Φ, p, and ε only.

Let $\{(b_1, b_2), (b_3, b_4)\}$ satisfy $b_1 b_4 - b_2 b_3 = 1$ and $\Phi(b_1, b_2) = \Phi(b_3, b_4) = c(\Phi)^{-1/2}$. Choose $\gamma \in \mathbb{R}$ such that

$$1 < \gamma < c(\Phi)^{1/2} (c(\Phi) - \varepsilon)^{-1/2}, \tag{15}$$

and put $(a_1, a_2) = \gamma(b_1, b_2)$, $(a_3, a_4) = \gamma^{-1}(b_3, b_4)$. Then $a_1 a_4 - a_2 a_3 = 1$ and $\Phi(a_1, a_2) = \gamma c(\Phi)^{-1/2}$, $\Phi(a_3, a_4) = \gamma^{-1} c(\Phi)^{-1/2}$. Let $m \geqslant m_0$ be an integer. By lemma 4.1 there exist a constant C_{10}, depending on Φ and ε only, and rational integers A_1, A_2, A_3, A_4 with $A_1 A_4 - A_2 A_3 = p^m$, such that

$$|A_i - a_i p^{m/2}| \leqslant C_{10}\, p^{4m/9} (\log p^m)^{7/9} \qquad (i = 1, 2, 3, 4).$$

It follows that there is a constant C_{11}, depending on Φ and ε only, such that

$$\begin{aligned} |\Phi(A_1, A_2) - p^{m/2} \gamma c(\Phi)^{-1/2}| &< C_{11}\, p^{4m/9} (\log p^m)^{7/9}, \\ |\Phi(A_3, A_4) - p^{m/2} \gamma^{-1} c(\Phi)^{-1/2}| &< C_{11}\, p^{4m/9} (\log p^m)^{7/9}. \end{aligned} \tag{16}$$

By (15) and (16), m_0 can be chosen so large that

$$\Phi(A_1, A_2) > \Phi(A_3, A_4), \tag{17}$$

and

$$\Phi(A_1, A_2) < p^{m/2} (c(\Phi) - \varepsilon)^{-1/2}. \tag{18}$$

Without loss of generality we may assume that $l = \mathrm{ord}_p(A_4)$ is minimal among the A_i $(i = 1, 2, 3, 4)$. Put $\alpha = A_3/A_4$, $(P, Q) = p^{-l}(A_1, A_2)$. Then $\alpha \in \mathbb{Z}_p$, and $p^{-l}(A_3, A_4)$, $(P, Q) \in \Gamma_{m-2l}$. By (17), (P, Q) is not a nearly Φ-best approximation to α. From (18) and

$$|P - Q\alpha|_p = |A_4^{-1} p^{-l}(A_1 A_4 - A_2 A_3)|_p = p^{-(m-2l)}$$

we infer (14). ∎

5. Strong Periodicity

In Section 2 we discussed periodicity of the sequence of approximation lattices of a p-adic integer α in the sense of the existence of a linear mapping that transforms approximation lattices into approximation lattices. Of course, such a mapping transforms bases into bases. In this section we demand for a given norm Φ that Φ-reduced bases are transformed into Φ-reduced bases.

Definition 5.1. Let $\alpha \in \mathbb{Z}_p$ and let Φ be a norm. The sequence of approximation lattices $\{\Gamma_m\}_{m=0}^{\infty}$ of α is said to be *strongly Φ-periodic* if there exist rational integers $k > 0$, $m_0 \geqslant 0$, a linear mapping $\Xi: \mathbb{R}^2 \to \mathbb{R}^2$, and Φ-reduced bases $\{(P_m, Q_m), (R_m, S_m)\}$ of Γ_m for all $m \geqslant m_0$, such that $\Xi(P_m, Q_m) = (P_{m+k}, Q_{m+k})$ and $\Xi(R_m, S_m) = (R_{m+k}, S_{m+k})$ for all $m \geqslant m_0$.

Strong periodicity obviously implies periodicity. Hence, by Theorem 2.1, it may occur only for rational and quadratic p-adic numbers α. Mahler [11] and Deanin [7] showed that strong Φ-periodicity may or may not occur for reduced elliptic norms Φ of discriminant -4 if α is elliptic, but that it does not occur if α is hyperbolic. In this section we prove that for hyperbolic α and for any norm Φ there is no strong Φ-periodicity, that for elliptic α there is at least one norm Φ for which strong Φ-periodicity does occur, and that for rational α it occurs at least for Φ_M and Φ_E. We need the following characterization of a Φ-reduced basis. The proof is left to the reader.

Lemma 5.1. *Let $\{(P, Q), (R, S)\}$ be a basis of the lattice Λ, and let Φ be a norm. Then this basis is Φ-reduced with (P, Q) as first successive minimal point if and only if for all $K \in \mathbb{Z}$*

$$\Phi(P, Q) \leqslant \Phi(R, S) \leqslant \Phi(R + KP, S + KQ).$$

Theorem 5.1. *Let p be prime. Let $F(X, Y) = aX^2 + bXY + cY^2$ be an elliptic form with $a, b, c \in \mathbb{Z}$, $a > 0$, such that $F(x, 1) = 0$ has a root $\alpha \in \mathbb{Z}_p$.*

Define the norm Φ *by* $\Phi(X, Y) = F(X, Y)^{1/2}$. *Then the sequence of approximation lattices* $\{\Gamma_m\}_{m=0}^{\infty}$ *of* α *is strongly* Φ*-periodic.*

Proof. Let Ξ, χ, ϕ, k, and h be as in the proof of Theorem 2.1. Let for $m = h+1, \ldots, h+k$ the Φ-reduced bases $\{(P_m, Q_m), (R_m, S_m)\}$ of Γ_m be given, and put

$$C_m = \begin{pmatrix} P_m & Q_m \\ R_m & S_m \end{pmatrix}.$$

Define $C_{m+k} = C_m \chi$ for all $m \geqslant h+1$. Then C_m corresponds to a basis $\{(P_m, Q_m), (R_m, S_m)\}$ for all $m \geqslant h+1$. It remains to show that these bases are all Φ-reduced. Put for all $m \geqslant h+1$

$$\begin{pmatrix} \alpha_m \\ \beta_m \end{pmatrix} = C_m \begin{pmatrix} 1 \\ -\alpha \end{pmatrix}.$$

Then it follows that $\alpha_{m+k} = \phi\alpha_m$, $\beta_{m+k} = \phi\beta_m$ for all $m \geqslant h+1$. Denote by $N(\xi)$ the norm of $\xi \in \mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Then

$$\Phi(P_{m+k}, Q_{m+k})^2 = aN(\alpha_{m+k}) = aN(\phi)\, N(\alpha_m) = N(\phi)\, \Phi(P_m, Q_m)^2,$$

$$\Phi(R_{m+k}, S_{m+k})^2 = aN(\beta_{m+k}) = aN(\phi)\, N(\beta_m) = N(\phi)\, \Phi(R_m, S_m)^2,$$

$$\Phi(R_{m+k} + KP_{m+k}, S_{m+k} + KQ_{m+k})^2 = aN(\beta_{m+k} + K\alpha_{m+k})$$

$$= aN(\phi)\, N(\beta_m + K\alpha_m) = N(\phi)\, \Phi(R_m + KP_m, S_m + KQ_m)^2$$

for all $K \in \mathbb{Z}$. The theorem follows by lemma 5.1 using induction. ∎

THEOREM 5.2. *Let* p *be prime. Let* $F(X, Y) = aX^2 + bXY + cY^2$ *be a hyperbolic form with* $a, b, c \in \mathbb{Z}$ *such that* $F(x, 1) = 0$ *has a root* $\alpha \in \mathbb{Z}_p$, $\alpha \notin \mathbb{Q}$. *Let* Φ *be any norm. Then the sequence of approximation lattices* $\{\Gamma_m\}_{m=0}^{\infty}$ *of* α *is not strongly* Φ*-periodic.*

Proof. Suppose the contrary. Then there exist

$$C_m = \begin{pmatrix} P_m & Q_m \\ R_m & S_m \end{pmatrix} \qquad (m = 1, 2, 3, \ldots),$$

$k, m_0 \in \mathbb{Z}$, $k > 0$, $m_0 \geqslant 0$, and a matrix χ with $\det(\chi) = p^k$ such that $C_{m+k} = C_m \chi$ for all $m \geqslant m_0$, and $\{(P_m, Q_m), (R_m, S_m)\}$ is a Φ-reduced basis of Γ_m for all m. Since

$$\chi^2 = \mathrm{Tr}(\chi)\chi - p^k I$$

we find that the sequence $\{C_{m_0+nk}\}_{n=0}^{\infty}$, hence also $\{P_{m_0+nk}\}_{n=0}^{\infty}$ satisfies the recurrence relation

$$u_{n+2} = \mathrm{Tr}(\chi) u_{n+1} - p^k u_n.$$

Let $\phi, \bar{\phi}$ be the eigenvalues of Ξ. They are real numbers, since F is hyperbolic. From $C_{m_0+2k} \equiv \mathrm{Tr}(\chi)\, C_{m_0+k} \pmod{p^k}$ it follows that $\phi + \bar{\phi} = \mathrm{Tr}(\chi) \neq 0$. By $\alpha \notin \mathbb{Q}$ we have $\phi \neq \bar{\phi}$. Thus we may assume $|\phi| < |\bar{\phi}|$. By $\phi\bar{\phi} = p^k$ we have $|\phi| < p^{k/2} < |\bar{\phi}|$. There exist $\lambda, \bar{\lambda} \in \mathbb{R}$ with

$$P_{m_0+nk} = \lambda\phi^n + \bar{\lambda}\bar{\phi}^n \qquad (n = 0, 1, 2, \ldots).$$

By $\phi, \bar{\phi} \notin \mathbb{Q}$ we have $\lambda \neq 0$, $\bar{\lambda} \neq 0$. It follows that

$$\lim_{n\to\infty} p^{-nk/2}\, |P_{m_0+nk}| = \lim_{n\to\infty} |\lambda(\phi/\bar{\phi})^n + \bar{\lambda}|\, |\bar{\phi} p^{-k/2}|^n = \infty \tag{19}$$

On the other hand, (P_m, Q_m) is a nearly Φ-best approximation to α. Put $\alpha_m = P_m - Q_m\alpha$. For $m \geqslant m_0$ we have $\alpha_{m+k} = \phi_1\alpha_m$, where ϕ_1 is the one of $\phi, \bar{\phi}$ with $\mathrm{ord}_p(\phi_1) = k$. Hence,

$$|P_{m_0+nk} - Q_{m_0+nk}\alpha|_p = p^{-nk}\, |P_{m_0} - Q_{m_0}\alpha|_p.$$

By Theorem 4.1(i) we have

$$\Phi(P_{m_0+nk}, Q_{m_0+nk}) \leqslant \frac{1}{\Delta(\Phi)^{1/2}\, |P_{m_0+nk} - Q_{m_0+nk}\alpha|_p^{1/2}} = Cp^{nk/2},$$

where C is independent of n. By the convexity of the norm Φ, this contradicts (19). ∎

THEOREM 5.3. *Let p be prime, and $\alpha \in \mathbb{Z}_p \cap \mathbb{Q}$. Let $\Phi = \Phi_M$ or $\Phi = \Phi_E$. Then the sequence of approximation lattices $\{\Gamma_m\}_{m=0}^{\infty}$ of α is strongly Φ-periodic.*

Proof. Put $\alpha = P/Q$, $P, Q \in \mathbb{Z}$, $\gcd(P, Q) = 1$. By considering $-\alpha$ in case $\alpha < 0$ we may assume $P, Q > 0$. Choose $R, S \in \mathbb{Z}$ with $PS - QR = 1$. For all sufficiently large m, (P, Q) is a first successive minimal point in Γ_m. Let

$$f_m(x) = \Phi(p^m R + Px, p^m S + Qx)$$

reach its minimum at $x = k_m$. Put $K_m = [k_m]$ if $f_m([k_m]) \leqslant f_m([k_m] + 1)$, and $K_m = [k_m] + 1$ otherwise. Put

$$(R_m, S_m) = p^m(R, S) + K_m(P, Q).$$

Then $\{(P, Q), (R_m, S_m)\}$ is a Φ-reduced basis of Γ_m for all sufficiently large m. Note that $k_m = pk_{m-1}$, hence $k_m = p^m k_0$. For $\Phi = \Phi_M$ we have

$$k_0 = -\frac{R+S}{P+Q},$$

for $\Phi = \Phi_E$ we have

$$k_0 = -\frac{PR+QS}{P^2+Q^2}.$$

In both cases, $k_0 \in \mathbb{Q}$. Hence the sequence $\{k_m - [k_m]\}_{m=0}^{\infty}$ is periodic, with period length n say. We claim that for Φ_E and Φ_M also the sequence $\{k_m - K_m\}_{m-0}^{\infty}$ is periodic with period n. For Φ_E, $f_m(x)^2$ is a quadratic polynomial, which is symmetric about k_m. Hence K_m is the nearest integer to k_m, and the claim follows immediately. For Φ_M, put

$$(R'_m, S'_m) = p^m(R, S) + [k_m](P, Q),$$
$$(R^*_m, S^*_m) = (R'_m, S'_m) + (P, Q).$$

It is easy to check that

$$\begin{aligned} \Phi_M(R'_m, S'_m) &= -R'_m, \\ \Phi_M(R^*_m, S^*_m) &= S^*_m. \end{aligned} \tag{20}$$

By the periodicity of $\{k_m - [k_m]\}_{m=0}^{\infty}$ we find that

$$(R'_{m+n}, S'_{m+n}) = p^n(R'_m, S'_m) + (1-p^n)([k_m] - k_m)(P, Q).$$

Also, by $k_m = p^m k_0 = -p^m(R+S)/(P+Q)$,

$$R'_m + S'_m = ([k_m] - k_m)(P+Q),$$

which depends only on the residue class of $m \pmod n$. Thus

$$R'_{m+n} + S^*_{m+n} = R'_m + S^*_m.$$

By (20) it follows that $\Phi_M(R'_{m+n}, S'_{m+n}) \leqslant \Phi_M(R^*_{m+n}, S^*_{m+n})$ if and only if $\Phi_M(R'_m, S'_m) \leqslant \Phi_M(R^*_m, S^*_m)$. Hence $\{k_m - K_m\}_{m=0}^{\infty}$ is periodic for $\Phi = \Phi_M$.

To complete the proof, note that for all large enough m

$$(R_{m+1}, S_{m+1}) = p(R_m, S_m) + J_m(P, Q)$$

with $J_m = K_{m+1} - pK_m = (K_{m+1} - k_{m+1}) - p(K_m - k_m)$ depending on $m \pmod n$ only. Put for m large enough

$$C_m = \begin{pmatrix} P & Q \\ R_m & S_m \end{pmatrix}, \psi_m = \begin{pmatrix} 1 & 0 \\ J_m & p \end{pmatrix},$$

then $C_{m+1} = \psi_m C_m$, and $\{\psi_m\}$ is periodic. By the remark following Definition 2.3, the sequence $\{\Gamma_m\}_{m=0}^{\infty}$ is strongly Φ-periodic. ∎

Remark. It seems likely that there is a large family of norms Φ for which strong Φ-periodicity occurs for rational α. Obviously there are norms for which the above method will not work, e.g., norms with $k_0 \notin \mathbb{Q}$.

ACKNOWLEDGMENTS

The author is greatly indebted to Professor R. Tijdeman and Dr. F. Beukers for their help and encouragement. He was supported by the Netherlands Foundation for Mathematics (SMC) with financial aid from the Netherlands Organization for the Advancement of Pure Research (ZWO).

REFERENCES

1. M. K. AGRAWAL, J. H. COATES, D. C. HUNT, AND A. J. VAN DER POORTEN, Elliptic curves of conductor 11, *Math. Comp.* **35** (1980), 991–1002.
2. S. I. BOREWICZ AND I. R. ŠAFAREVIČ, "Zahlentheorie," Birkhäuser Verlag, Basel/Stuttgart, 1966.
3. J. BROWKIN, Continued fractions in local fields I, *Denomstratio Math.* **11** (1978), 67–82.
4. P. BUNDSCHUH, p-adische Kettenbrüche und Irrationalität p-adischer Zahlen, *Elem. Math.* **32** (1977), 36–40.
5. J. W. S. CASSELS, "An Introduction to the Geometry of Numbers," Springer-Verlag, Berlin/Göttingen/Heidelberg, 1959.
6. A. A. DEANIN, A counterexample to a conjecture of Mahler on best P-adic diophantine approximation constants, *Math. Comp.* **45** (1985), 621–632.
7. A. A. DEANIN, Periodicity of P-adic continued fraction expansions, preprint, Villanova Univ., Villanova, Pa., 1984.
8. M. HARRINGER, "Kettenbruchentwicklung quadratischer Funktionen," Dissertation, Köln, 1981.
9. R. T. GREGORY AND E. V. KRISHNAMURTHY, "Methods and Applications of Error-free Computation," Springer-Verlag, New York, 1984.
10. K. MAHLER, Zur Approximation p-adischer Irrationalzahlen, *Nieuw Arch. Wisk. (2)* **18** (1934), 22–34.
11. K. MAHLER, On a geometrical representation of p-adic numbers, *Ann. of Math.* **41** (1940), 8–56.
12. K. MAHLER, "Lectures on Diophantine Approximations I: g-adic Numbers and Roth's Theorem," Univ. of Notre Dame Press, Notre Dame, Ind., 1961.
13. TH. SCHNEIDER, "Über p-adische Kettenbrüche," *Symposia Math.*, No. IV, pp. 181–189, Academic Press, London/New York, 1978.
14. R. TIJDEMAN, Approximation of real matrices by integral matrices, *J. Number Theory* **23** (1986), 65–69.
15. P. S. WANG, M. J. T. GUY, AND J. H. DAVENPORT, P-adic reconstruction of rational numbers, *SIGSAM Bull.* **16** (1982), 2–3.